NATIONAL DEFENSE UNIVERSITY

NATIONAL WAR COLLEGE

THREAT WARNING FOR AMERICA'S CRITICAL INFRASTRUCTURES

PAUL W. THRASHER/CLASS OF 2000
COURSE 5605
SEMINAR K

FACULTY SEMINAR LEADER:
COL TOM SMITH

FACULTY ADVISOR:
DR. DAVID ROSENBERG

Report Documentation Page

Form Approved
OMB No. 0704-0188

Public reporting burden for the collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing the collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden, to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington VA 22202-4302. Respondents should be aware that notwithstanding any other provision of law, no person shall be subject to a penalty for failing to comply with a collection of information if it does not display a currently valid OMB control number.

1. REPORT DATE	2. REPORT TYPE	3. DATES COVERED
2000	**N/A**	**-**

4. TITLE AND SUBTITLE	5a. CONTRACT NUMBER
Threat Warning for America's Critical Infrastructures	5b. GRANT NUMBER
	5c. PROGRAM ELEMENT NUMBER
6. AUTHOR(S)	5d. PROJECT NUMBER
	5e. TASK NUMBER
	5f. WORK UNIT NUMBER
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES) **National Defense University National War College Washington, DC**	8. PERFORMING ORGANIZATION REPORT NUMBER
9. SPONSORING/MONITORING AGENCY NAME(S) AND ADDRESS(ES)	10. SPONSOR/MONITOR'S ACRONYM(S)
	11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION/AVAILABILITY STATEMENT
Approved for public release, distribution unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT

15. SUBJECT TERMS

16. SECURITY CLASSIFICATION OF:			17. LIMITATION OF ABSTRACT	18. NUMBER OF PAGES	19a. NAME OF RESPONSIBLE PERSON
a. REPORT	b. ABSTRACT	c. THIS PAGE			
unclassified	**unclassified**	**unclassified**	**UU**	**15**	

Introduction[1]

The President's Commission on Critical Infrastructure Protection, *Critical Foundations*, was a report of a multi-agency effort to "study the critical infrastructures that constitute the life support systems of (the United States), determine their vulnerabilities, and propose a strategy for protecting them in the future".[2] Spurred by this report, the President signed Presidential Decision Directive 63 which built upon the PCCIP's recommendations. In signing PDD-63, the President's intent was for the United States to "take all necessary measures to swiftly eliminate any significant vulnerability to both physical and cyber attacks on our critical infrastructures, including especially our cyber systems".[3]

One of the goals of PDD-63 was to create a national center to warn of significant infrastructure attacks, to include the detection and analysis of such attacks, with maximum participation from the private sector. This task fell to the FBI's National Infrastructure Protection Center (NIPC) to provide threat assessment, warning, vulnerability assessment, and law enforcement investigation and response.[4] Now, nearly two years hence, these encompassing tasks are largely going undone while the NIPC focuses nearly all its resources on law enforcement investigation and response, with only minor Information Sharing and Analysis Center (ISAC) coordination. It is the purpose of this paper to show that national cyber threat warning measures

---

[1] Direct quotes are appropriately footnoted. Much of the content of this paper has been developed from lectures, question and answer sessions, visits, and interviews with multiple sources; including: National Information Protection Center, Information Technology Association of America, iDefense, National Security Council (NSC), NSC Office of Science and Technology Policy, National Coordinating Center for Telecommunications, Information Operations Directorate of the Joint Chiefs of Staff, Office of Assistant Secretary of Defense for C3I, Deputy Assistant Secretary of Defense for Security and Information Operations, Joint Task Force for Computer Network Defense, and the Defense Information Systems Agency. Particular appreciation is provided to Mr. William Gravell of TRW who provided detailed insight to the needs for a cyber National Indications and Warning Center during an interview 9 March 2000.

[2] President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructure," October 1997, p. i.

[3] "The Clinton Administration's Policy on Critical Infrastructure Protection," White Paper on Presidential Decision Directive 63, May 22, 1998

[4] *ibid.*

are important for protecting critical infrastructures. Further, this paper asserts that tactical and strategic cyber threat warning is inadequate and needs to be reassessed vis-à-vis the role of the Department of Defense, the Intelligence Community, and the Justice Department.

Background

Providing threat warning, or Indications and Warning (I&W), of impending attack or military threat to the United States has long been the responsibility of the Department of Defense (DOD) and Intelligence Community (IC). These threats have, up to now, resided outside the borders of the United States and have been physical or kinetic in nature. Forces massing, foreign warships off the coast of the U.S., intercontinental ballistic missiles, and regional adversaries blocking U.S. access to vital resources are all threats to the U.S. vital interests that the public understands and not only expects, but demands, the DOD and IC to provide proper predictive warning against.

The additional threat the U.S. must prepare for today makes that statement no longer true. Today, the United States must also protect herself from the threat of critical infrastructure electronic attacks conducted by adversaries who are able to move virtually within and across the borders of the United States, complicating and clouding the responsibilities and legal roles of the DOD and IC. To properly warn of this type of threat means the DOD and IC would have to conduct traditional information gathering and analysis in ways that the public would not only vehemently oppose, but which would also be illegal.

By giving the Justice Department the responsibility to provide cyber-attack threat warning information, the Clinton Administration placed an important part of cyber-defense within an agency without the culture, background, ability, or public support to accomplish it. As evidence, the NIPC has yet to issue any cyber threat warning information in the two years of their existence.

Worse, the NIPC has been largely criticized for their lack of coordination with private industry and sharing of post-attack profiles and information with other government agencies or private businesses. The culture of the NIPC, which their actions to date confirm, is to use the information they gain concerning unauthorized cyber or electronic intrusions for the primary purpose of building a criminal case for prosecution within the courts. While this is an important and needed part of the overall defense of critical infrastructures, it runs counter to sharing information for the purpose of predicting and warning others of impending attacks. Like the DOD and IC, the Justice Department would also be seen as violating civil rights should they ever take the steps necessary to provide encompassing threat warning information.

Vulnerabilities and Threats

To understand why an I&W system for cyber-attacks is important, it is necessary to first understand the vulnerabilities of and threat to the critical infrastructure. The vulnerability to electronic computer network attack comes from depending on linked systems that share common networks and accesses. Commonly called hacking, the impact of intrusions into infrastructures can be devastating no matter if the attack was part of a malicious cyber-terrorist plot; criminals exploiting trade secrets, laundering money, or conducting theft or fraud; a foreign government conducting Information Warfare (IW) intent on disrupting or destroying U.S. resources and emergency systems; "professional" hackers adding another notch on their cyber-intrusion belt; or novice teenagers joy-riding on the Information Superhighway without realizing they are breaking the law. Protection of the nation's critical infrastructures has to account for all these actors, as well as the continuing vulnerabilities to disgruntled employees, equipment failure, and system administrators' ineptitude. Providing predictive and useful threat warning information of an attack

from all these potential sources becomes difficult and complicated as the areas of responsibility for each of these threats cross many agencies and are bound by multiple legal statutes.

If the only threat to our critical infrastructures were from teenaged information highway joy-riders, then protection of our nation's critical infrastructures would take a very different approach. Unfortunately, the General Accounting Office reported an alarming 250,000 attempted attacks (during 1998) on military computers, which cost millions of dollars to track and repair.[5] Although those numbers have been doubted by critics, what is not doubted is that the number of intrusions and information system denial-of-service attacks targeted against government computers has increased, and there have been some very successful hacks. Michael McConnell, former Director of NSA and now a vice president at Booz Allen & Hamilton, has said that, "the required skill level of hackers is going down as there are more sophisticated tools available freely on the Internet, and that means there are more people who can do harm".[6]

Are there actors who will deliberately attempt to infiltrate into U.S. computer systems to disrupt or deny service to authorized users? We must remember too that one of the critical infrastructures is the Finance and Banking sector, which may be less susceptible to the motives of denial or disruption, but nonetheless vulnerable to intrusions for criminal purposes. You do not need to look far for sobering examples of infiltration. Mr. Michael Vatis, Deputy Director of the FBI and the Chief of the NIPC, reported to Congress that, "A 1998 study by the Computer Security Institute shows that 64% of companies polled reported information system security breaches – an increase of 16% over (1997). The total financial losses from the 241 organizations that could put a dollar figure on them add up to $136,822,000. This figure represents a 36% increase in reported losses over the 1997 figure of $100,115,555 in losses." He further reported, "A 1996 survey by the

[5] Richard Mullins, "FBI Eyes Net Crime," San Francisco Examiner, http://www.examiner.com/daily/0426hack.html
[6] *ibid.*

American Bar Association of 1,000 companies showed that 48 percent had experienced some form of security compromise in 1997, with the highest percentage of intrusions (57%) occurring in the banking and finance industry."[7]

So how much of a threat is there and what is the risk from the threat? While Director of the CIA, John Deutch told Congress in 1997 that he ranked Information Warfare as the second most serious threat to U.S. national security, just below weapons of mass destruction in terrorist hands.[8] John Serbian, Chief of the CIA's Critical Technologies Group reported that, "As Director of Central Intelligence George Tenet testified before the Senate Select Committee on Intelligence in January (1999) and more recently again in June before the Senate Governmental Affairs Committee, we have identified several countries, based on all-source intelligence information, that have government-sponsored information warfare programs." Mr. Serbian further stated, "The battlespace of the Information Age will extend to our domestic infrastructure. Our electric power grids and our telecommunications networks could be targets of the first order. An adversary capable of implanting the right offensive tool, or accessing the right computer system, can cause extensive damage."[9]

There are many that argue all this talk about threats and vulnerabilities is nothing more than government and specific business industries creating an unfounded panic in order to garner money or tighten government controls on the public's freedoms. While the opponents need to be heard, I contend that the government's warning should be taken

---

[7] Cybercrime, Transnational Crime, and Intellectual Property Theft Statement for the Record of Michael A. Vatis, Deputy Assistant Director and Chief, National Infrastructure Protection Center, Federal Bureau of Investigation, before the Congressional Joint Economic Committee, March 24, 1998

[8] C. Paul Robinson, Joan B. Woodard, and Samuel G. Varnado, "Critical Infrastructure: Interlinked and Vulnerable," Issues in Science and Technology Online, Fall 1998, http://www.sandia.gov/CIS/issues.htm

[9] "CIA Official Assesses Information Warfare Threat," 10 December 1998, http://www.usia.gov/current/news/latest/98121001.plt.html?/products/washfile/newsitem.shtml

seriously. Consider these cases presented by Louis J. Freeh, Director of the FBI, during a speech 4 March 1997.

> "Someone with a lap top computer sitting in an apartment in St. Petersburg, Russia, intruded into a bank and attempted to move millions of dollars out of accounts to a place where they can be exploited.
>
> A young man sitting in his own apartment (in Sweden), hacked his way across the Atlantic Ocean into U.S. telephone switching systems and worked his way down to Northern Florida, where over the course of several weeks, he interfered with 911 systems and had the capability to disable the system.
>
> (Consider) a recent terrorism case where an individual maintained plans in his lap top computer to attack airliners and other targets."[10]

Certainly, these examples show the potential damage that could be done by a properly motivated individual or nation-state. While the example of the terrorist plans to attack airliners was a cyber-crime only in the sense that his planning information was encrypted and kept on a personal computer, I find that case particularly interesting. The President's Commission on Critical Infrastructure Protection (PCCIP) reported in October 1997 that they found, as of then, "information-based attacks cannot cause trains and planes to crash, nor are they likely to cause pipelines to rupture. Tomorrow – perhaps next year, perhaps in ten years – critical transportation systems could be vulnerable to such attacks and crippled unless action is taken now."[11] That proved to be a very short-sighted statement since just five months later the FBI was conducting a plea bargain in Massachusetts with a teenage hacker who managed to break into the former NYNEX (now Bell Atlantic) system, and through it, disable telecommunications at a regional airport, cut off services to the airport's control tower, and prevent incoming planes from turning on

[10] Louis J. Freeh, speech to the 1997 International Computer Crime Conference, March 4, 1997.
[11] PCCIP, p. A-15.

runway lights.[12] It is not hard to imagine the catastrophe this could cause should the same action occur at one of the nation's leading airports. The more realistic and practical effect of electronic cyber-attack, however, is short of catastrophe. But the use of these tools can obviously result in delaying or confusing the transportation and logistics of U.S. forces forward deployed, or disrupt the provision of vital services at home.

Indications and Warning

If the critical infrastructures of the U.S. are subject to a threat of attack and need protecting, then a system is required that would identify the indicators and provide the warning that an attack is likely. Although directed as a task for the NIPC within PDD-63, that warning system does not completely exist today. Warning must also be conducted within a specific timeframe in order to be useful. The timing of the warning will differ depending on when indicators become known. For the purposes of this paper, I will term tactical warning that warning provided when an attack is just beginning or ongoing, and strategic warning that warning provided sufficiently in advance of an attack so that defensive, preventative, or preemptive measures can be employed.

Mr. William Gravell identifies two central questions for employing I&W: 1) What is to be protected, and 2) Against what threats do we need to protect ourselves? To answer these questions, he provides an I&W model that considers: Vulnerability (how an attack could be conducted); Modeling (what would be the necessary precursors of an attack); Sensors (built keyed to expected observables), Analysis (resolution of sensory input); Awareness (heightened stakeholder understanding of threats and vulnerabilities); Agreements (information sharing arrangements); and Architecture (information dissemination).[13] Each of these factors are

[12] Cybercrime, Transnational Crime, and Intellectual Property Theft Statement for the Record, March 24, 1998.
[13] William Gravell, "Some Observations Along the Road to 'National Information Power'", Duke Journal of Comparative and International Law, Spring 1999, p.426, http://www.law.duke.edu/journals/djcil/

important when considering a comprehensive I&W system. Three are particularly pertinent to this discussion; vulnerability (already discussed), sensors, and analysis.

Tactical warning that a cyber attack is beginning or on-going should be easy to provide, logically, but is realistically very difficult. The ability to recognize the patterns and factors which would indicate an attack is underway requires real-time monitoring of all the information systems' sensors within each critical infrastructure sector. Although certain individual agencies and private businesses do a good job of this, it is only accomplished, sector-wide, within the DOD and IC.

Each service, at DOD direction, has taken the steps to monitor the activities on their own classified and unclassified systems in ways that indicate, and automatically block, unauthorized intrusion or service disruption attempts. Any attempted intrusion or attack is reported within service channels as well as to the Joint Task Force for Computer Network Defense (JTF-CND). JTF-CND is located with the Defense Information Systems Activity and is able to continuously remain aware of the technical health of the entire DOD network. This allows them to provide tactical warning information to Space Command (CINC tasked with CND), DOD, and the services. For tactical warning, the DOD has proven it is the model for the rest of the infrastructure sectors to emulate.

This expertise within DOD came at great expense in monitoring and sensing equipment and personnel cost; a cost that industry and the other infrastructure sectors either don't see as necessary or are unwilling to pay. Also, the culture of the military encourages the sharing of information to provide for a common defense. That concept does not translate well for industry, who sees no advantage to sharing intrusion information with their competitors, share holders, or government.

PDD-63 called for Information Sharing and Analysis Centers (ISAC) to be established for each critical infrastructure sector. Of the two ISACs that have stood-up, Global Integrity for the

Banking & Finance sector and National Coordinating Center for the Telecommunications sector, neither has a mechanism in place to provide real-time network and intrusion monitoring. Part of the reason for this has to do with expense and investment. But part of the reason also has to do with a concern of ultimate government monitoring, a la "big brother", of their networks since the end-game design is to have all the ISACs sharing information among themselves and with government. But other reasons within industry are concerns over government not being able to protect their shared information under Freedom of Information Act rules, and the undesired potential for participating in unfair competitive practices as defined within the Fair Labor Standards Act.

It is only fair to point out that the same industry ISACs that are poor at tactical warning do a reasonable job at post-event analysis, reporting, and coordination within and among industry and government. But conducting this type of post-analysis is akin to closing the barn door after the cows have escaped. If the infrastructure sectors are poor at tactical warning, then certainly they make up for it through strategic warning? Unfortunately, as hard as tactical warning is, strategic warning poses even more challenges and the ISACs haven't even begun to consider them.

Strategic warning is more complicated than tactical warning because strategic warning must determine adversary intent and make reasonable predictions on the likelihood of the adversary carrying out his intent. Assessments must be made concerning whether adversaries exist, if they possess the means to attack, whether they possess the skills and will to attack, the method of attack, and timeframe the attack will take place.

The DOD and IC has, again, historically been reasonably successful with this type of I&W against conventional threats and has, over time, created a comprehensive I&W infrastructure that supports impressive modeling and analysis so that predictive warning is credible. The DOD and

IC also have an important strategic cyber warning role. The problem is that the DOD and IC cannot provide warning against all threats. Since anyone with a computer and INTERNET access is a potential threat, I am choosing to ignore those attackers who are unknown until they actually conduct an attack, even though that is a very serious I&W problem all its own. But even when choosing to not factor the risk of unknown actors as a threat, the DOD and IC are still unable to provide strategic warning against the remaining potential threats.

Consider the group of potential attackers mentioned earlier: cyber-terrorists, criminals, nation states, "professional" hackers, and teenaged joy-riders. A proper I&W system needs to provide strategic warning against all these actors since they all pose some level of threat; the tools used and vulnerabilities exploited by one actor are the same for all. While the DOD and IC have a clear role in providing strategic warning against any of these actors residing outside U.S. borders, they cannot conduct the intelligence and analysis activities necessary to provide warning against actors within U.S. borders; even when (like one recent real-world example) a foreign national convinced unwitting U.S. citizens to aid him in an attack.

Again the question becomes, who is providing strategic threat warning for private industry and the infrastructure sectors? Certainly NIPC has a role, but it is limited to conducting criminal investigations for law enforcement purposes. The ISACs, on the other hand, should be interested in strategic warning, but have not begun to even consider all the steps necessary to conduct predictive threat warning. They are overwhelmed in just conducting post-attack and vulnerability analysis and reporting. Interestingly, however, there are private businesses emerging in a new market who are offering to provide this type of service to private business customers.

One such business is iDefense, a company that conducts hardware and software analysis for customers to provide them with vulnerability assessments in order to repair or minimize them.

They also track incident data and provide typical ISAC-style post-attack analysis and information sharing.[14] The attraction for industry is that they have more confidence that a private business such as iDefense will be able to protect their proprietary data better than the government. But iDefense is taking their services one step further than other similar companies by conducting "intelligence" activities within hacker chat rooms and other open-source forums; functions the IC is prohibited from conducting. They then use that information to warn customers of impending attacks. While still in a beginning stage, their efforts have resulted in several companies being warned of various levels of information attacks by as much as 24-48 hours. That is certainly far enough in advance for system administrators to take steps to better protect their systems. There is a problem, however, with claiming predictive warning as a service product of business. Like traditional I&W, it is difficult to provide cyber threat warning intent for all adversaries or for all attack methods. Any success in this area may prove to be only minor and temporary. So since strategic cyber threat warning may not enjoy a high degree of success by any single group or agency, the question becomes as to whether it should be attempted at all, and if so, against what type of threat?

Proposals and Conclusion

So what needs to be done to improve strategic cyber threat warning? The answer appears simple, but is actually difficult. Mr. Gravell summed it up into this statement, "the government needs to determine and publish its vital national information interests."[15] Easily said, hard to do in a reasonable manner that identifies the exact information infrastructures and systems that need to be defended and protected like all other vital U.S. interests.

[14] Dan Owen, interview by author 16 March 2000, iDefense
[15] William Gravell, interview by author 9 March 2000, TRW

Take the example of the cyber attack actors again. As currently written, all cyber attacks are federal crimes. This means that the unwitting teenaged joy-rider can be held to the same level of criminal liability as a cyber-terrorist intent on damaging a power distribution system. But both of these actions do not involve the same level of threat to the vital interests of the U.S. Developing a better definition and understanding of vital national information interests has several benefits:

> It identifies and gets buy-in from the government and industry as to what the vital interests truly are.
>
> It focuses the DOD and IC on providing an assessment of whether our vital interests can actually be threatened through cyber means, and if so, provides a priority for countering the threat.
>
> With industry buy-in, they become more willing to share cyber and proprietary information with the government concerning vital interests.
>
> It prioritizes for the government what is and is not important when requesting industry cooperation and information sharing.
>
> It prioritizes cyber law enforcement efforts.
>
> It permits laws to be changed which would reduce the criminal liability of inconsequential cyber attacks while simultaneously permitting the development of response tools and methods when vital interests are challenged.

In conclusion, Indications and Warning of cyber threats, as for all threats, are vital to understanding and preventing attacks against the critical infrastructure of the United States. Cyber I&W efforts, unfortunately, are lacking and there are no foreseen measures being undertaken to improve them. The one organization tasked with cyber threat warning, NIPC, is not culturally or organizationally positioned to provide cyber I&W, and more importantly, share that information with a wide audience in a way that would be useful. The DOD and IC, who are more adept at I&W are prohibited from conducting certain activities against U.S. citizens within the borders of the U.S. A true, complete, comprehensive I&W framework will actually have to rely on all

participants and stakeholders, including private industry. In order for industry to participate and have buy-in, it is important that the government not make all cyber attacks equal or categorize all information requirements as vital. Instead, the true vital information interests of the U.S. need to be identified and published to coalesce unity of effort towards assessing and ameliorating those cyber threats to the vital interests. In doing so, strategic threat warning becomes more focused and limited resources can be placed against those infrastructures where tactical threat warning would continue to be needed. The benefit of which will be a more responsive government-industry partnership able to predict, identify, and warn of the increased likelihood of cyber attack for prevention and mitigation purposes, as envisioned in PDD-63.

Bibliography

"CIA Official Assesses Information Warfare Threat," 10 December 1998, http://www.usia.gov/current/news/latest/98121001.plt.html?/products/washfile/newsitem.shtml

"The Clinton Administration's Policy on Critical Infrastructure Protection," White Paper on Presidential Decision Directive 63, May 22, 1998.

Freeh, Louis J., speech to the 1997 International Computer Crime Conference, March 4, 1997.

Gravell, William, "Some Observations Along the Road to 'National Information Power'," Duke Journal of Comparative and International Law, Spring 1999, http://www.law.duke.edu/journals/djcil

Gravel, William. Interview by author 9 March 2000, TRW

Mullins, Richard, "FBI Eyes Net Crime," San Francisco Examiner, http://www.examiner.com/daily/0426hack.html

Owen, Dan. Interview with author 16 March 2000, iDefense

President's Commission on Critical Infrastructure Protection, "Critical Foundations: Protecting America's Infrastructure," October 1997

Robinson, C. Paul, Woodard, Joan B., and Varnado, Samuel G. "Critical Infrastructure: Interlinked and Vulnerable," Issues in Science and Technology Online, Fall 1998, http://www.sandia.gov/CIS/issues.htm

Vatis, Michael A., Cybercrime, Deputy Assistant Director and Chief, National Infrastructure Protection Center, Federal Bureau of Investigation, Transnational Crime, and Intellectual Property Theft Statement before the Congressional Joint Economic Committee, March 24, 1998